KU LEUVEN

ICRI Working Paper Series

The evolving role of the individual under EU data protection law

Brendan Van Alsenoy

ICRI Working Paper 23/2015

Interdisciplinary Centre for Law and ICT, KU Leuven

icri

10 August 2015

The evolving role of the individual under EU data protection law

Brendan van Alsenoy[1]

[1] Brendan Van Alsenoy is a legal researcher at ICRI/CIR, KU Leuven – iMinds. His research focuses on data protection, privacy, intermediary liability and trust services.

Abstract

The role of individuals has shifted. In less than 30 years, individuals have transcended their role as passive "data subjects" to become actively involved in the creation, distribution and consumption of personal data. Unless an exemption or derogation applies, individuals are – at least in theory – subject to data protection law. This hypothesis was confirmed early on by the *Lindqvist* ruling and more recently in *Ryneš*. The aim of this paper is to analyse whether it is still possible to reconcile the "personal use exemption" of article 3(2) Directive 95/46 with the widespread use of technologies by individuals. Using online social networks, drones and Google Glass as use cases, this paper will explore how the personal use exemption might be shaped in order to preserve individuals' ability to use new technologies freely, while still protecting the privacy interests of others.

Keywords: data protection, roles and responsibilities, personal use, social media, drones, Google Glass

1. The evolving role of the individual[2]

We use information and communication technologies every day. Mobile devices tell us where to eat, who to meet and how to get there. We share pictures, post videos and tweet reviews. We google everything and everyone. We are non-stop creators, publishers and consumers of data.[3]

In a just few years, the introductory paragraph to this paper will be hopelessly dated. "*We used to worry about stuff people posted on Facebook*" they'll say. Or that running a name search on Google "*is just sooo 2014*". "*Today we worry about seamless connectivity between personal and environmental sensors, real-time use of facial recognition and other forms of augmented reality*". Celebrated authors such as David Brin[4] and Jonathan Zittrain[5] have been alluding to such scenarios for years. While certain prophecies are yet to be fulfilled, this much is clear: the role of individuals has shifted. In less than 30 years, individuals have transcended their role as passive "data subjects" to become actively involved in the creation, distribution and consumption of personal data.[6]

Data protection laws have traditionally targeted governmental and commercial institutions as the main subjects of regulation.[7] The reason is simple: computer usage started out as a prerogative of large companies, governments, and universities.[8] As a result, the first generation of data protection laws was geared towards data usage by resourceful public and private sector organizations.[9] Although they have been revised several times

[2] Title inspired by the Agenda of the 2010 OECD Conference, "The Evolving Role of the Individual in Privacy Protection: 30 Years After the OECD Privacy Guidelines", Jerusalem, 25-26 October 2010, accessible at http://www.oecd.org/internet/ieconomy/46252465.pdf (last accessed 17 January 2015).

[3] See also O. Tene, "Privacy: The new generations", *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 21-25.

[4] See e.g. D. Brin, *The Transparent Society*, Basic Books, Lexington, 1998, p. 4-10.

[5] J. Zittrain, *The Future of the Internet— And How to Stop It*, 2008, Yale University Press, New Haven & London, 342 p, accessible at http://futureoftheinternet.org/files/2013/06/ZittrainTheFutureoftheInternet.pdf (last accessed 4 February 2015).

[6] OECD, *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, 2013, Paris, p. 32, available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (last accessed 12 January 2015).

[7] J. Zittrain, *The Future of the Internet— And How to Stop It*, *o.c.*, p. 200.

[8] See e.g. J. Bing, "Data protection in a time of changes", in W.F. Korthals Altes a.o. (eds.), *Information Law Towards the 21st Century*, 1992, Deventer, Kluwer Law and Taxation Publishers, p. 247-248. For discussion of the availability and main forms of usage of computer systems in the 1970's see Commission des Communautés Européens, "Systèmes à grande puissance de traitement automatique de l'information. Besoins et applications dans la Communauté européenne et au Royaume-Uni vers les années soixante-dix", *Études*, Série Industrie, n° 6, 1971, p. 39-57.

[9] See also V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", in P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, 1998, London, MIT Press, p. 223 and C. Reed, 'The Law of Unintended Consequences - Embedded Business Models in IT Regulation', *Journal of Information Law and Technology* 2007, vol. 2, paragraph 33, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/reed/reed.pdf (last accessed 17 January 2014).

since, it seems difficult to fully dispense with certain implicit assumptions.[10] Meanwhile, advances in information and communication technologies have fundamentally altered the context in which data protection laws are to be applied. The new reality is at odds with the framing of roles and responsibilities in many legal instruments, including Data Protection Directive 95/46.[11]

Under Directive 95/46, individuals are viewed mainly as the "beneficiaries" of protection. If an individual decides to process data relating to others, however, he or she will be considered a "controller" rather than a "data subject".[12] Unless an exemption or derogation applies, he or she will – at least in theory – be subject to the full panoply of data protection norms. This hypothesis was confirmed early on by the *Lindqvist*[13] ruling and more recently in *Ryneš*[14]. Central to both cases was the question of whether the processing activities of an individual fell within the scope of article 3(2) of Directive 95/46, which exempts processing "*by a natural person in the course of a purely personal or household activity*". The answer, in both instances, was a resounding "no". For some time now, scholars have been asking whether the "all or nothing" approach of article 3(2) makes sense.[15] Is data protection really the right way right to think about church newsletters or home security systems? Should we perhaps revise the scope article 3(2) so that "non-commercial" activities fall outside the scope of data protection law?[16]

Data protection advocates are cautious when it comes to expanding the notion of "personal use". For all its benefits, the widespread availability of ICTs also enables individuals to inflict considerable privacy harms. Outing a sexual preference[17], broadcasting a traumatic experience[18], public shaming[19] or posting "revenge porn"[20] are all just a few clicks

[10] See also M. Birnhack, 'Reverse Engineering Information Privacy Law', *Yale Journal of Law and Technology* 2012, Vol. 24, p. 64 et seq. and C. Reed, 'The Law of Unintended Consequences - Embedded Business Models in IT Regulation', *l.c.*, in particular paragraphs 26 through 39.

[11] See also OECD, 'The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines', *l.c.*, p. 27.

[12] The scope of this paper does not include individuals who are acting on behalf of a group or organisation. In such cases, it is the group or organisation which will considered the "controller", whereas the individual making the decision will generally be viewed simply as its agent.

[13] European Court of Justice, *Bodil Lindqvist*, C-101/01, 6 November 2003, available at www.curia.eu..

[14] Court of Justice of the European Union, *František Ryneš v. Úřad pro ochranu osobních údajů*, C‑212/13, 11 December 2014, accessible at www.curia.eu.

[15] See in particular R. Wong and J. Savirimuthu, "All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet", 25 *J. Marshall J. Computer & Info. L.* 2008, 241-266; B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', Identity in the Information Society (IDIS) 2009, p. 75-76 and N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *Computer Law Review International (Cri)* 2010, Vol. 4, 104 et seq.

[16] See e.g. D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *International Law & Management Review* 2010, Vol. 6, 150.

[17] See e.g. High Court of Justice, *Applause Store Productions Limited and Matthew Firsht v. Grant Raphael*, 24 July 2008, [2008] EWHC 1781 (QB), accessible at www.bailii.org.

[18] See e.g. Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – deposit ail 3 febbraio 2014, sentenza n. 5107/14, accessible at available at www.dirittoegiustizia.it

[19] High Court of Justice, Stephen Robins and Gabbitas Robins v. Rick Kordowski and Tim Smee, 22 July 2011, [2011] EWHC 1912 (QB), accessible at www.bailii.org.

away. While traditional civil law remedies (e.g., defamation, breach of confidence, right to control the use of one's image, misuse of private information) may offer a solution, certain remedies show limitations when applied to the online context.[21] Data protection laws could provide an important legal backstop in such cases. At the same time, the application of data protection laws to individuals acting in a private capacity also raises questions. Should we subject private individuals to the same regulatory logic as organisations? Can we expect average citizens to familiarize themselves with the intricacies of data protection law? Do the rules even make sense when applied to the context of social interaction?

The central thesis of this paper is that the time has come to broaden the personal use exemption. It will start by tracing the legislative history of article 3(2) and its subsequent interpretation by the European Court of Justice. Next, it will contrast the current approach to the *ratio legis* of Directive 95/46 as a whole, which was designed to regulate organisations rather than individuals. The paper will go on to analyse several existing proposals to revise the personal use exemption. Using three use cases, the paper will then evaluate whether the current proposals adequately address the evolving role of individuals. Two criteria will serve as guiding principles during the evaluation, namely the principle of legal certainty and principle of proportionality.[22] There is no special justification for employing these criteria, other than that they are both general principles of EU law. Other general principles of EU law (such as the principles of subsidiarity or fairness) may also be relevant, but fall outside the scope of this paper.

---

[20] See http://www.endrevengeporn.org/.

[21] See e.g. D. Erdos, 'Filling Defamation's Gaps: Data Protection and the Right to Reputation', Oxford Legal Studies Research Paper 2013, No. 69, available at https://www.repository.cam.ac.uk/bitstream/handle/1810/245805/OA1491_Reputation%20and%20Data%20Protection%20Article_Final_title.pdf?sequence=4 (last accessed 17 January 2015).

[22] Legal certainty requires laws to be sufficiently precise so as to allow individuals to reasonably foresee its consequences See e.g. J.R. Maxeiner, "Legal certainty: a European alternative to American legal indeterminacy?", *Tulane Journal of International and Comparative Law* 2007, Vol.15(2), p. 549. Proportionality, on the other hand, requires that laws are suitable, necessary and non-excessive. See e.g. T.-I. Harbo, "The function of the proportionality principle in EU law", *European Law Journal* 2010, Vol.16(2), p. 165.

2. The exemption for "purely personal" or "household" activity

2.1 Article 3(2) of Directive 95/46

The second indent of article 3(2) provides that Directive 95/46 shall not apply to the processing of personal data carried out

"*by a natural person in the course of a purely personal or household activity*".

a. Legislative history

The personal use exemption was not an original creation of the drafters of Directive 95/46. The 1978 French Data Protection Act had already exempted "non-automated or mechanized" processing if it was intended purely for personal use.[23] The 1984 UK Data Protection Act exempted individuals if the processing "c*oncerned only the management of his personal, family or household affairs*" or if the data were held "*for recreational purposes*".[24] The European Commission's proposal contained similar language, by providing that the Directive would not apply to "*files held by an individual solely for private and personal purposes*".[25] Shortly after submission, the Committee on the Environment, Public Health and Consumer Protection proposed modifying the text to read as follows:

> "*This Directive shall not apply to files held by an individual for the purpose of purely personal or household activities*"[26]

---

[23] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC. A comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and The Netherlands and their impact on the private sector*, Kluwer, Deventer, Computer/Law Series n° 6, 1990, p. 82. The exemption was said to encompass 'non-professional' files, which are 'not related to any activity which places those that hold them in an "organisational" relationship [*rapport organique*] with third parties' (A. Holleaux, 'La loi du 6 Janvier 1978 sur l'informatique et les libertés (I)', *La Revue Administrative* 1978, Vol. 31, n° 181, p. 165). *Automated* processing of personal data by individuals would, strictly speaking, fall within the remit of the Act, even if it were carried out for a purely private purpose. (N. Lenoir, 'La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des liberté: Éléments pour un premier bilan de cinq années d'activité, *La Revue adminstrative* 1983, Vol. 36, no. 215, p. 465).

[24] Section 33(1)) of Data Protection Act, 1984 c. 35. A copy scanned copy of the original 1984 UK Data Protection Act is accessible at http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf. See also House of Lords (HL) Debates (Deb), 10 March 1983, vol. 440 c. 373. Strictly speaking, data held for private purposes was only partially exempted from the 1984 Data protection act (see section 33(1). In principle, the users of these data still needed to comply with the general principles of data protection contained in Section 1 of the act. However, in practice there was a total exemption as the principles were only enforceable against registered data users. (A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 118 footnote 21.)

[25] Commission of the European Communities, "Proposal for a Council Directive concerning the processing of individuals in relation to the processing of personal data", COM(90) 314 final, SYN 287, 13 September 1990, p. 51.

[26] Committee on the Environment, Public Health and Consumer Protection, "Amendments to the draft opinion of the Commission proposal for a Council directive on the protection of individuals in relation to the processing of personal data (Com(90) 314 final – C3-323/90 – SYN 287", 10 May 1991, amendment n° 23.

Wordsmithing aside, the personal use exemption would remain essentially unchanged throughout the remainder of the legislative process. Recital (12) would add two examples of personal or household activities, namely "*correspondence and the holding of records of addresses*."[27]

b. Ratio legis

The explanatory memorandum accompanying the Commission proposal offered the following rationale for article 3(2):

> "*Paragraph 2 provides for exceptions where invasions of privacy are unlikely to occur […] because the data are used for private purposes only, as is the case in with a personal electronic diary […]*".[28]

Similar risk-based considerations were present in paragraph 3(b) of the 1980 OECD Privacy Guidelines. Paragraph 3(b) stated that the Guidelines should not be interpreted as preventing "*the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties*". Its accompanying Memorandum made clear that "*the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (e.g. personal notebooks)*".[29]

The legislative history of Directive 95/46 offers little further guidance. The terms "purely" and "exclusively" clearly indicate that article 3(2) was to be construed narrowly. No standard was provided, however, to determine what might or might not constitute a "personal" or "household" activity.[30] As a result, it was up to the European Court of Justice (ECJ) to clarify the scope of the personal use exemption.

2.2 Lindqvist

Mrs. Lindqvist, who worked as a catechist in a local parish, had set up a number of web pages. The pages included information about several other parishioners, who were referenced either by their full names or merely by their first names. In many cases telephone numbers were listed. The pages also described, "in a mildly humorous manner" the jobs held by the parishioners and their hobbies. Of one parishioner it was stated that she had injured

[27] Recital (12) Directive 95/56 (emphasis added)

[28] Commission of the European Communities, Proposal for a Council Directive concerning the processing of individuals in relation to the processing of personal data, *l.c.*, p. 21.

[29] OECD, *Explanatory Memorandum to the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, paragraph 43. Article 9(3) of Convention 108 also recognized the possibility for exemptions in cases where there was "no risk of an infringement of the privacy of the data subjects", but only in relation to statistics or scientific research.

[30] B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 72.

her foot and was working half-time for medical reasons. Mrs. Lindqvist had not obtained the consent of the individuals concerned. She had also failed to notify the data protection authority. She was subsequently prosecuted for violation of the Swedish law on personal data.[31]

As to the question of whether the activities of Mrs. Lindqvist were covered by the exception for personal use, the ECJ replied that the exemption must be interpreted as

> "*relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*".[32]

The ECJ thus put forth two criteria to determine whether the personal use exemption applies. In the first place the processing activity must be carried out "*in the course of private and family life*". Secondly, the exemption shall not apply where data are published on the internet and made accessible to an "*indefinite number of people*".

The first component of the *Lindqvist* test is perhaps the most striking. Whereas article 3(2) of the Directive exempts data processing in the context of "*purely personal or household*" activities, the ECJ referred to activities carried out "*in the course of private or family life*". The latter wording is nowhere to be found in the text of Directive 95/46. The word choice instead seems to have been inspired by the language of article 7 of the EU Charter and/or article 8 of the European Convention of Human Rights.[33] The allusion to this terminology appears to have been intentional. If so, it arguably has important ramifications for the scope of the personal use exemption. It has long been established that the protection of "private life" under article 8 ECHR is not restricted to that which has historically been dubbed "the private sphere". Rather, the European Court of Human Rights has repeatedly underlined that it also protects a right to identity and personal development, and the right to establish and develop relationships with others.[34]

The second part of the *Lindqvist* test precludes its application in cases where data are made available to an "indefinite" number of people, yet does not specify a limit or threshold. The second part of the *Lindqvist* test is arguably most problematic[35], as will be made evident by the use cases presented in section 5.[36]

---

[31] European Court of Justice, *Bodil Lindqvist*, Case C-101/01, at paragraphs 12-15.

[32] European Court of Justice, *Bodil Lindqvist*, at paragraph 47 (emphasis added).

[33] Article 8(1) ECHR provides that "Everyone has the right to respect for his *private and family life*, his home and his correspondence". Article 7 of the EU Charter provides that "Everyone has the right to respect for his or her *private and family life*, home and communications."

[34] See e.g. European Court of Human Rights, *P.G. and J.H. v. United Kingdom*, 25 September 2001, application no. 44787/98 at 56 and European Court of Human Rights, *Niemietz v. Germany*, 16 December 1992, application no. 13710/88, at 29.

[35] See also R. Wong and J. Savirimuthu, "All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet", p. 246 ("*The ECJ's decision clarifies the extent to which individuals may be able to benefit from Article 3(2), when placing personal information on the Internet, however, it raises several questions. If it is accepted that limiting access of an individual's Web page to family*

2.3 Ryneš

Ryneš concerned the use of video surveillance for home security purposes. For a number of years, Mr. Ryneš had been plagued by attacks by unknown persons. The windows of the family home had been broken on several occasions.[37] In order to protect his family and home, Mr. Ryneš decided to install a camera system. It consisted of one fixed camera which monitored the entrance to his home, as well as the public footpath and the entrance to the house opposite.[38] Almost immediately, the camera system served its purpose. On the second night after its installation, one of the windows of Mr. Ryneš's home was broken by a shot from a catapult.[39] The video recording made it possible to identify two suspects, which eventually led to criminal proceedings.[40]

When petitioned by one of suspects, the Czech Data Protection Authority (DPA) held that Mr. Ryneš's camera system violated the Czech data protection act.[41] The main reasons were that (1) the camera system had captured, without consent of the individuals concerned, the images of people moving along the street or entering the house opposite; (2) Mr. Ryneš had failed to provide the individuals concerned any information regarding the processing of their personal data; and (3) Mr. Ryneš had failed to report the camera system to the DPA.[42] Further legal proceedings ensued, resulting in a reference for a preliminary ruling to the ECJ. Could the processing carried out by Mr. Ryneš be classified as the processing of personal data "by a natural person in the course of a purely personal or household activity"?

The ECJ concluded that Mr. Ryneš's processing activities did not fall within the remit of article 3(2). [43] It reasoned that

---

members will be exempt from Article 3(2) DPD, such that the Data Protection Directive 95/46/EC does not apply, where does one draw the line for individuals whose web pages may extend beyond family members?"); E. C. Harris, "Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have All the Answers", 22 *Am. U. Int'l L. Rev.* 2007, p. 787 and F.J. Garcia, "Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators", 15 *Fordham Intell. Prop. Media & Ent. L.J.* 2005, p. 1232 et seq.

[36] Cf. *infra*; section 5.1.

[37] Court of Justice of the European Union, *František Ryneš v. Úřad pro ochranu osobních údajů,* 11 December 2014, Case C-212/13, at paragraph 14.

[38] *Ibid*, at paragraph 13. The ECJ noted that the recording capabilities of the camera system were limited in several respects: "*[t]he system allowed only a visual recording, which was stored on recording equipment in the form of a continuous loop, that is to say, on a hard disk drive. As soon as it reached full capacity, the device would record over the existing recording, erasing the old material. No monitor was installed on the recording equipment, so the images could not be studied in real time. Only Mr Ryneš had direct access to the system and the data*."(*Id.*)

[39] *Ibid*, at paragraph 15.

[40] *Ibid*, at paragraph 15.

[41] Ibid, at paragraph 16.

[42] *Ibid*, at paragraph 16.

[43] Ibid, at paragraph 35.

> "*To the extent that video surveillance such as that at issue in the main proceedings covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46.*"[44]

In reaching its conclusion, the ECJ also took into account that (a) the objective of Directive 95/46 is to ensure a high level of protection[45]; (b) any derogations and limitations must apply only in so far as is strictly necessary[46]; and (c) the very wording of article 3(2) ("purely") also suggests it should be narrowly construed[47].

The ECJ recognized that the mere fact that the processing "incidentally" concerns the private life of other persons does not necessarily preclude application of article 3(2).[48] After all, recital (12) of the Directive mentions "correspondence and the holding of records of addresses" as examples. By definition, such processing activities "incidentally concern" the private life of other persons. The continuous monitoring of a public space, however, is something different. If a camera is directed "*outwards from the private setting*", it regularly affects individuals with whom the controller has no personal or household relationship.

The *Ryneš* Court concluded its reasoning by considering the practical implications of its ruling. Although it was not asked to pronounce itself on the legality of Mr. Ryneš's video surveillance system, it did note that:

> "*[T]he application of Directive 95/46 makes it possible, where appropriate, to take into account — in accordance, in particular, with Articles 7(f), 11(2), and 13(1)(d) and (g) of that directive — legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the case in the main proceedings.*"[49]

In other words: even if the personal use exemption does not apply, the applicability of the requirements of Directive 95/46 does not by itself render a home security system unlawful.[50] Directive 95/46 recognizes the "legitimate interest"[51] of the controller as a possible justification for the processing of personal data (in other words: consent is not necessarily required). The Directive also allows Member States to exempt controllers from

---

[44] Ibid, at paragraph 33.
[45] Ibid, at paragraph 27
[46] Ibid, at paragraph 28-29.
[47] Ibid, at paragraph 30.
[48] Ibid, at paragraph 32.
[49] Ibid, paragraph 34.
[50] Advocate-General Jääskinen in fact concluded that the processing at issue would be lawful under Directive 95/46 (see Opinion of Advocate-General Jääskinen, František Ryneš v Úřad pro ochranu osobních údajů, Case C-212/13, 10 July 2014, at paragraphs 63 et seq. See also pdpEcho, "CJEU: CCTV camera in family home falls under the Data protection directive, but it is in principle lawful", 11 December 2014, accessible at http://pdpecho.com/2014/12/11/cjeu-cctv-camera-in-family-home-falls-under-the-data-protection-directive-but-it-is-in-principle-lawful/ (last accessed 16 March 2015).
[51] See article 7(f) Directive 95/46.

their duty to inform in cases where "the provision of such information proves impossible or would involve a disproportionate effort".[52] Finally, article 13(1) allows for additional derogations (a.o. to the principles of data quality and data subject rights) where such measures are necessary (a) for the prevention or detection of criminal offences[53] or (b) to protect the data subject or of the rights and freedoms of others[54].

The conceptual approach outlined by the *Ryneš* Court suggests that Directive 95/46 can (and should) be implemented in such a way that it does not unduly restrict individuals' ability to pursue a legitimate objective. It is up to the Member States, however, to actually provide for appropriate derogations.[55] A significant number of Member States have already introduced specific rules governing the use of CCTV, including by private individuals.[56] Beyond CCTV, however, it seems only few States have introduced specific derogations.[57] Without ruling out the possibility such derogations may still be introduced, it is worth reflecting whether data protection requirements should be applied to private individuals. The next section will contrast the conceptual approach of the ECJ in *Ryneš* to the *ratio legis* of Directive 95/46 as a whole, which was designed to regulate organisations rather than individuals.

[52] See article 11(2) Directive 95/46.
[53] Article 13(1)d Directive 95/46.
[54] Article 13(1)g Directive 95/46.
[55] The latest draft of the proposed Data Protection Regulation likewise leaves the matter to be addressed by the Member States. Article 21 of the "compromise text" of the European Parliament allows for derogations similar to article 13. See European Parliament, Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)) Compromise amendments on Articles 1-29, 7 October 2013, accessible at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf (last accessed 16 March 2015). The compromise text does not allow, however, to introduce exemptions to e.g., data quality principles (article 5), the documentation requirement (article 28), data breach notifications (article 31) or international transfers (articles 40 et seq).
[56] See D. Korff, *EC Study on Implementation of Data Protection Directive 95/46/EC*, Study Contract ETD/2001/B5-3001/A/49, 2002, 135 et seq., accessible at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667
[57] Idem.

3. Directive 95/46 is geared towards organizations

Data protection laws originally emerged as a response to concerns regarding the increased use of computing applications by public and private sector organisations.[58] Even though Directive 95/46 was enacted more than 20 years after the first data protection laws appeared, many of its requirements still reveal an organisational mind set.[59] The organisational mind set of Directive 95/46 is evident in both the language and substance of its provisions.

3.1 A focus on data management

A key provision of Directive 95/46 is article 6, which defines "principles relating to data quality". As currently defined, these principles contain principles of "good data management", rather than guidelines for data use by private individuals. For example, article 6(1) specifies that personal data must be:

- *collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*;
- *adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*;
- *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified*;
- *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.*"

The Directive's focus on data management is not surprising if one considers the genealogy of European data protection law. The first generation of data protection laws were motivated – at least in part – by a desire to improve the integrity of *organizational*

[58] See V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", in P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, 1998, London, MIT Press, p. 221; F.W. Hondius, *Emerging data protection in Europe*, North-Holland Publishing Company, Amsterdam, 1975,, p. 7; P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerpen, Intersentia, 2006, p. 77.

[59] See also See also C. Reed, 'The Law of Unintended Consequences - Embedded Business Models in IT Regulation', *l.c.*, paragraph 36 et seq.

decision-making.[60] As computers made it easier to store information for prolonged periods of time, the risk of harms resulting from the reliance upon erroneous data was expected to increase.[61] Several data protection requirements can be seen as efforts to "*sanitize the informational environment*"[62]; in particular those provisions which impose limits upon the collection and storage of information, or provisions which require that recorded information be kept up-to-date or limit the use of such data to a particular context.[63]

3.2 Procedural nature

A second indication that Directive 95/46 is geared towards organizations is the *procedural nature* of many of its safeguards.[64] The drafters of the first data protection laws feared that the use of computing technologies would render organizational decision-making increasingly opaque.[65] People's wellbeing would depend on the outcome of obscure data processing practices, without any ability to contest them (or even being aware of them).[66] As a result, data protection laws came to introduce a set of procedural safeguards designed to act as "checks" against potential misuse of personal data.[67] Specifically, safeguards were designed to promote *transparency* of processing and the *accountability* of organizations.[68] The duty to inform, the right of access and the creation of dedicated administrative oversight are clear examples. The argument that there is a need for similar "checks" against misuse of personal data by private individuals is far less compelling, as the power relationships between private individuals are fundamentally different from those between individuals and organizations.[69] Moreover, applying the procedural mechanisms of Directive 95/46 to individuals also raises questions of proportionality. As Zittrain observes:

---

[60] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca, 1992, p. 44; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, 2002, The Hague, Kluwer Law International, Information Law Series, p. 105 et seq..

[61] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 35. See e.g. A.R. Miller, "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society", *l.c.*, p. 1114.

[62] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 137.

[63] *Id.*

[64] See P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in, *Privacy and the Criminal Law*, ed. E. Claes, A. Duff and S. Gutwirth (Antwerpen/Oxford: Intersentia, 2006), p. 76 et seq.

[65] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 103 and 107; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 19 and 29; J. A. Cannataci, *o.c.*, p. 60 and 64.

[66] See also L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 94-95.

[67] See also S. Rodotà, "Data Protection – Some problems for Newcomers", in Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, 1983, Rome, Camera dei Deputati, p. 188..

[68] See also J. Alhadeff, B. Van Alsenoy and J. Dumortier, 'The accountability principle in data protection regulation: origin, development and future directions', in D. Guagnin, L. Hempel, C. Ilten a.o. (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, Houndmills (UK), 2012, p. 49-82

[69] OECD, *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, *o.c.*, p. 32. See also J.

"*It is one thing to ask a corporation to disclose the personal data and records it maintains; it is far more intrusive to demand such a thing of private citizens. Such disclosure may itself constitute an intrusive search upon the citizen maintaining the records.*"[70]

3.3 Resource constraints

Compliance with Directive 95/46/EC requires expertise and resources which are typically only available to organizations.[71] For example, ensuring confidentiality and security of processing requires people trained in IT security. The duty to notify supervisory authorities or to draft contracts implies access to legal counsel. While a single individual may have the skills and resources to perform each of these functions, it seems more realistic that they would be observed by organizational departments or outside contractors. In other words: a mismatch exists between the legal obligations of "controllers" and social practices of individuals. Not only does it appear impractical to apply several of the Directive's provisions to private individuals, it would also be excessively burdensome and unrealistic.[72]

Zittrain, o.c., p. 216 ("*There is a quantum difference between a police officer and the little old lady (or other tourist or private citizen) videotaping or photographing a public event.*")

[70] J. Zittrain, o.c., p. 222.

[71] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 104.

[72] Ibid, p. 104 et seq. and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', 131 et seq. and p. 149. See also See also J. Zittrain, o.c., 221 ("[…] *the sorts of administrative burdens we can reasonably place on established firms exceed those we can place on individuals--at some point, the burden of compliance becomes so great that the administrative burdens are tantamount to an outright ban*."

4. Towards a more balanced approach?

Policymakers have not been immune to the issues highlighted in the previous section. During the past five years, three of the main international instruments of data protection regulation have been subject to review. This section will analyse how two of these instruments have tried to address the evolving role of individuals.

4.1 The Revised OECD Privacy Guidelines

Preparations for the review of the OECD Privacy Guidelines began in 2010, in the context of the Guidelines' 30th anniversary.[73] As part of the process, the OECD organized a thematic event dedicated to the "evolving role of the individual".[74] In a subsequent report, it was highlighted that

> "*The concept of data controller […] did not necessarily contemplate the possibility of individuals acting in a manner similar to data controllers with respect to the personal data of others, a development that has been triggered by the emergence of Web 2.0. […] Given the key role that individuals play in transmitting personal data […] further consideration may need to be given to their role in privacy protection frameworks*.'[75]

In 2011, the OECD's Working Party for Information Security and Privacy formed a Volunteer Group of Privacy Experts ("Expert Group").[76] In the end, the Expert Group was unable to reach a consensus on how to address the evolving role of individuals. Certain members felt it would be appropriate to address this issue within the revised Guidelines. Others felt quite strongly that the Guidelines themselves should not address the practices of individuals. In the end, it was decided to merely highlight the issue in the Supplemental Explanatory Memorandum, which provides:

> *"Over the past few years, individuals have […] become actively involved in creating, posting and sharing personal data about themselves, friends, relatives and others, over a vast array of information outlets including social networking services […]. When discussing this change, it was recognised that not every actor should necessarily be regulated in the same way. For example, individuals acting in the*

[73] OECD, *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, *o.c.*, p. 11.

[74] See e.g. OECD, 'The Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines', International Convention Center, Jerusalem, Israel, 25-26 October 2010, available at http://www.oecd.org/sti/ieconomy/46252465.pdf (last accessed 24 February).

[75] OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers* 2011, No. 176, OECD Publishing, p. 27-28, available at http://dx.doi.org/10.1787/5kgf09z90c31-en (last accessed 8 February 2015).

[76] OECD, *Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Paris, 2011, DSTI/ICCP/REG(2011)4/FINAL, p. 6, accessible at http://www.oecd.org/sti/ieconomy/48975226.pdf. The Expert Group focused on three main themes, namely: (1) the roles and responsibilities of key actors; (2) geographic restrictions on transborder data flows; and (3) proactive implementation and enforcement. (*Ibid*, 11).

context of their private lives are generally perceived to fall outside the remit of the Guidelines, as relationships among individuals are usually fundamentally different from those between individuals and organisations. Non-legislative measures, including education and awareness raising, were considered more appropriate to address the privacy risks associated with the activities of individuals. Where an individual does cause damage to the privacy interests of others, tort or civil law may offer a possible remedy, but other measures may need to be considered as well."[77]

4.2 The Draft Regulation

a. Commission Proposal

In January 2012, the European Commission outlined its proposals for reforming the 1995 Data Protection Directive.[78] The accompanying draft Regulation[79] did not propose significant changes to the scope the personal use exemption. Article 2(2)d provided that the Regulation was not to apply to the processing of personal data

"*by a natural person without any gainful interest in the course of its own exclusively personal or household activity*"

Other than the addition of the words "without any gainful interest", the Commission's proposal essentially left the language of article 3(2) untouched. Draft recital (15) specified that

"*This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity*".

b. Statement by the Article 29 Working Party

In February of 2013, the Article 29 Working Party issued a Statement on the "current discussions" surrounding the data protection reform. One of the annexes accompanying the

[77] OECD, *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, *o.c.*, p. 32.

[78] European Commission, *Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Affairs Committee and the Committee of the Regions, COM(2012) 9 final, 25 January 2012, accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en (last accessed 8 February 2015).

[79] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD), 25 January 2012, accessible at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed 8 February 2015).

Statement concerned the future of the personal use exemption.[80] In the Statement, the Working Party considered that

> "*the current Directive's approach to personal or household processing has an unrealistically narrow scope that no longer reflects individuals' capacity to process data for personal and household activities and has therefore become anachronistic*."[81]

As an alternative approach, the Working Party proposed using the following five criteria to determine whether or not the personal use exemption applies:[82]

(1) *Publicity*: is the data disseminated to an indefinite number of persons or to a limited community of friends, family members or acquaintances?
(2) *Data subjects involved* is the data about individuals who have a personal or household relationship with the person posting it?
(3) *Scale and frequency*: does the scale and frequency of the processing suggest a professional or full-time activity?
(4) *Concerted action*: is the individual acting alone or is there evidence of individuals acting together in a collective and organized manner?
(5) *Adverse impact*: what is the potential adverse impact on individuals, including intrusion in their privacy?

None of these criteria would, by themselves, necessarily exclude application of the personal use exemption.[83] Instead, one should look at them in combination to determine whether, on the whole, the personal use exemption applies.[84] The proposed criteria would afford data protection authorities a certain degree of discretion when deciding whether or not to take action against a particular processing activity. At the same time, using the identified criteria would promote objectivity in this decision-making process.[85]

The Article 29 Working Party also took note of the Commission's proposal to insert the wording "without gainful interest" in article 2(2)d of the Regulation. In this respect it considered that

> "*WP29 assumes that the reference to 'gainful interest' is meant to make it clear that the processing of personal data done for the purposes of commercial activity does not fall within the exemption. […] WP29 fully accepts the intention of the wording. However, there is no doubt that individuals can engage in activity that results in*

[80] Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", 27 February 2013, p. 2, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf (last accessed 16 February 2015).
[81] *Ibid*, p. 2.
[82] *Ibid*, p. 4.
[83] *Id*.
[84] *Id.*
[85] *Id.*

'gainful interest' but can do so in a purely personal capacity. The example [...] where an individual sells their unwanted birthday presents on an e-commerce site is an obvious example of 'personal' gainful interest."[86]

c. Legislative scrutiny

In January 2013, the Parliamentary Committee on Civil Liberties, Justice and Home Affairs (LIBE) published its first official report on the proposed Regulation.[87] In its report, the LIBE Committee proposed striking the words "without any gainful interest" from the proposed text of article 2(2).[88] In May 2013, the European Council went even further by proposing to also strike the word "exclusively".[89] In the Council version, the Regulation would not apply to the processing of personal data

"*by a natural person (...) in the course of (...) a personal or household activity*"[90]

The European Parliament, however, has held on to a more narrow understanding of the personal use exemption. In the "compromise text", released in October 2013, article 2(2)d reads as follows:

"*(d) by a natural person in the course of an exclusively personal or household activity. The exemption shall also apply to a publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons*"[91]

---

[86] *Ibid*, p. 8

[87] Prior to its first official report, the European Parliament published an external report which also analysed the scope of the personal use exemption in the Commission's proposal. See European Parliament, Directorate-General for Internal Policies, Policy Department A: Economic and Scientific Policy, *Reforming the Data Protection Package*, IP/A/IMCO/ST/2012-02, PE 492.431, September 2012, at p. 33, accessible at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492431/IPOL-IMCO_ET%282012%29492431_EN.pdf (last accessed 8 February 2015).

[88] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2012/0011(COD), Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) 16 January 2013, amendment 79, p. 62, accessible at http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE501.927 (last accessed 16 March 2015).

[89] Council of the European Union, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Key issues of Chapters I-IV, 2012/0011 (COD), 10227/13 ADD, 31 May 2013, p. 37, accessible at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010227%202013%20ADD%201 (last accessed 16 March 2015).

[90] *Id.*

[91] See European Parliament, Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)) Compromise amendments on Articles 1-29, 7 October 2013, p. 4, accessible at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-

The European Parliament thus seems to cling to the "indefinite number of people" test established by *Lindqvist*. It also retains the term "exclusively", which favours a narrow understanding of the personal use exemption. To date, the Council has not, however, revised its earlier stance.[92]

d. Evaluation

In my opinion, the approach advanced by the Council of Europe is the most salient. Omitting the word "exclusively" encourages a broader understanding of the personal use exemption, thereby already mitigating the risk of overregulation considerably. The Council text might still, however, be usefully complemented by the recommendations made by the Article 29 Working Party in its 2013 Statement. After all, the criteria proposed by WP29 can offer useful guidance when determining whether or not a certain activity may be considered as a "personal or household" activity. In other words: the Working Party criteria would help to promote legal certainty, while still preserving a much needed degree of flexibility.

Going one step further, however, one could also consider substituting the wording "*in the course of a personal or household activity*" by "*in the context of an individual's private or family*" (i.e. the first component of the *Lindqvist* test). Such a change would clarify that any activities related to the development of one's personal identity or the establishment of relationships with others shall in principle fall within the remit of the personal use exemption. The WP29 criteria would then simply identify the "tipping point" when additional limitations become justified in order to prevent undue interference with the rights and interests of others. The following section will present three use cases to explore the potential impact of the proposed changes in comparison to current state of play.

29/comp_am_art_01-29en.pdf. The same text was adopted again by the European Parliament on 12 March 2014.

[92] (d) by a natural person (...) in the course of (...) a personal or household activity (last verified 8 August 2015). It should be noted, however, that the Article 29 Working Party and the EDPS now advocate to retain the word "purely" or "exclusively" in order to limit favour narrow interpretation. See Article 29 Working Party, Appendix – Core topics in view of the trilogue, 17 June 2015, p. 3, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary.pdf and European Data Protection Supervisor, Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations, 27 July 2015, p. 7, accessible at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf (last accessed 8 August 2015)

5. Use cases

5.1 Online social networks

Online Social Networks (OSNs) allow us to engage with potentially unlimited audiences. What was previously the prerogative of publishers, companies or "geeks", is now at everyone's fingertips. Sadly, the use of OSNs can also bring about serious privacy harms. Inadvertent disclosures, breaches of confidence and reputational damage are but a few examples of social networking gone wrong.

a. Users as "controllers"

Every OSN user, at least in theory, acts as a "controller" when processing data about others.[93] The control exercised by an OSN user in principle extends to any processing operations he or she initiates voluntarily (i.e., without solicitation). For example, a company that uses an OSN for purposes of product promotion shall be considered a controller towards:

- any personal data that is included on the company's profile page (including its list of "connections" or "friends");
- any personal data which the company collects through the OSN (e.g., personal attributes of connections);
- any information about individuals which the company disseminates through the OSN.[94]

b. Implications of *Lindqvist*

In *Lindqvist*, the ECJ put forward two tests to determine whether the personal use exception can be applied. First, the processing activity must be carried out *"in the course of private and family life*". Second, the exception shall not apply where data are published on the Internet and made accessible to an indefinite number of people. The first test suggests that private OSN users, who make use of an OSN for purposes of social interaction, should in principle be able to benefit from the personal use exemption. After all, social interaction is

[93] B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 70; Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', WP 163, 12 June 2009, p. 5; R. Wong, "Social networking: a conceptual analysis of a data controller", Communications Law Vol. 14, No. 5, 2009, p. 143 et seq.; N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 102 et seq; P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *Computer Law & Security Review* 2010, Vol. 26, p. 537-538; and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *International Law & Management Review* 2010, Vol. 6, p. 131 et seq.

[94] See also Information Commissioner's Office (ICO), 'Social networking and online forums – when does the DPA apply?', 24 May 2013, Version 1.0, p. 3, accessible at https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf (last accessed 18 March 2015).

an essential component of one's private or family life.[95] The second criterion, however, entails that the exemption shall not apply where data are made accessible to an indefinite number of people. This implies that certain OSN users will be unable to invoke article 3(2) once the data in question passes a certain threshold of accessibility.[96]

c. Position of the Article 29 Working Party

In its 2009 Opinion on social networking, the Article 29 Working Party implied that the processing activities of private OSN users are generally covered by the personal use exemption.[97] Since then, several scholars have argued that in practice there are many instances in which the exemption cannot be applied.[98] In its 2013 Statement, the Article 29 Working Party recognized the undesirable consequences of the current state of affairs and called for a more nuanced approach:

> "*[…] WP29 finds it difficult to accept that the fact that an individual makes his blog or her social networking profile available to the world at large is – in itself – a factor that means that any processing of personal data done in connection with* [sic] *necessarily falls outside the scope of personal or household processing.*
>
> *However, WP29 recognises that making information available to the world at large should be an important consideration when assessing whether or not processing is being done for personal purposes. However, this should not in itself be considered determinative*."[99]

d. Evaluation

In cases where the personal use exemption does not apply, the OSN user in question shall in principle be subject to the same requirements as those incumbent upon controllers in any other context. This outcome is warranted where organizations are concerned, who make use of OSNs to realize their commercial, political or other objectives. This outcome is problematic, however, where individuals acting in a private capacity ("private individuals")

---

[95] B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 74.

[96] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 103.

[97] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 5. The Working Party did identify two situations in which the exemption does not apply. First, the exception does not apply if the individual is acting 'on behalf of a company or association, or uses the [OSN] mainly as a platform to advance commercial, political or charitable goals.' Second, the exception for personal use also does not apply if the individual 'takes an informed decision to extend access beyond self-selected "friends"'. (*Id.*)

[98] See e.g. P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *l.c.*, p. 540; N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 101 et seq. and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *l.c.*, p. 147 et seq..

[99] Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.*, p. 9

are concerned. If an OSN user is subject to data protection law, it implies, inter alia, that this OSN user is required to ensure:

(1) *legitimacy* of processing (article 7);
(2) *transparency* of processing (article 10-11);
(3) respect for the *data quality* principles such as fairness, proportionality, finality and accuracy (article 6);
(4) that *data subjects* have the ability to exercise certain rights (article 12 and 14);
(5) *confidentiality and security* of processing (article 16-17);
(6) that, where required, *notification* to national supervisory authorities is performed (article 18).

At first glance, it seems as if a number of these requirements could be applied to private individuals in a reasonable and proportionate way. For example, many would agree that "friends" should refrain from uploading pictures of one and other without their approval.[100] Or that they should not post inaccurate or harmful statements, regardless of whether their profile is set to "private" or not. For other data protection requirements, however, there exists a mismatch between legal provisions and OSN practices. For example, how does one interpret the requirement of not keeping personal data in identifiable form for longer than is necessary (art. 6(1)e) in relation to OSN users? Is it possible to determine a reasonable time-span as to how long a user should be allowed to maintain a picture or remark relating to another person on his profile page? Should we be requiring individuals to make such a determination? Another problematic provision is the controller's duty to inform.[101] Should OSN users be required to formally notify their peers of (1) their identities; (2) the purposes of the processing of their personal data as well as (3) the (categories of) recipients concerned? Or is it sufficient if these things are understood implicitly, as a result of prevailing social norms and common OSN practices?

The criteria proposed by the Article 29 Working Party in its 2013 Statement could lead to a fundamentally different outcome. Individuals engaging in social networking in the context of their private lives would be able to benefit from the personal use exemption, regardless of the number of recipients involved. While certain forms of OSN use might still fall outside the personal use exemption, it is clear that users acting in a private capacity would generally be exempt from complying with formal data protection requirements as such.

[100] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 104. Others may find it perfectly acceptable (and even enjoyable) to find themselves 'tagged' unexpectedly in a picture uploaded by a shared contact.
[101] See also D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *l.c.*, p. 132.

5.2 Drones

a. Civilian use of drones

Drone use by civilians is on the rise. Judging by the headlines, a drone might soon be dispatching your online purchases[102], bringing food to your table[103], or buzzing around your neighbourhood just for fun[104]. While most Europeans are yet to see drones in action, the European Commission insists on the importance enabling the introduction of drones on the EU Market.[105] On 8 April 2014, the Commission adopted a Communication entitled "*A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*".[106] According to the Communication, the market for Remotely Piloted Aircrafts ("RPAs" or "drones") offers enormous potential for economic growth and jobs.[107] The absence of an appropriate regulatory framework and the lack of harmonization are seen as major obstacles for the development of a European market for RPAs.[108] The regulatory framework should, of course, take into account the fundamental rights of citizens and RPA operators would need to comply with applicable data protection provisions.[109]

b. Position of the European Data Protection Supervisor

In November 2014, the European Data Protection Supervisor (EDPS) issued an Opinion in response to the Commission's Communication. As a preliminary observation, the EDPS noted that many uses of RPAs will involve processing of personal data:

> "*[M]any RPAS that will be introduced on the market will include a video camera device with specialised software to process the video feed. This camera device with its specialised software may well have capabilities such as high power zoom, facial*

[102] L. Kelion, "Alibaba begins drone delivery trials in China", BBC News Technology, 4 February 2015, accessible at http://www.bbc.com/news/technology-31129804 (last accessed 16 March 2015).
[103] T. Wong, "Drone waiters to plug Singapore's service staff gap", BBC News Technology, 8 February 2015, accessible at http://www.bbc.com/news/world-asia-31148450 (last accessed 16 March 2015)
[104] L. Sydell, "As Drones Fly In Cities And Yards, So Do The Complaints", NPR Blog, 12 May 2014, http://www.npr.org/blogs/alltechconsidered/2014/05/12/311154242/as-drones-fly-in-cities-and-yards-so-do-the-complaints
[105] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner"", 26 November 2014, paragraph 5, accessible at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-11-26_Opinion_RPAS_EN.pdf (last accessed 10 February 2015).
[106] European Commission, Communication from the Commission to the European Parliament and the Council, "A new era for aviation Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", Brussels, 8 April 2014, COM(2014) 207 final, accessible at http://ec.europa.eu/transport/modes/air/doc/com%282014%29207_en.pdf
[107] *Ibid*, p. 3.
[108] *Ibid*, p. 4.
[109] *Ibid*, p. 7-8.

recognition, behaviour profiling, movement detection, or number plate recognition. RPAS could also be equipped with Wi-Fi sensors, microphones and audio recording systems, biometric sensors processing biometric data, GPS systems processing the location of the person filmed, or systems reading IP addresses of all devices located in a building over which the RPAS will fly. Embedded technologies could also include the possibility to track devices carrying RFID chips and persons/vehicles wearing them"[110]

The EDPS also considered the applicability of Directive 95/46 to the use of RPAs for private activities, in particular by hobbyists.[111] It concluded that

"*In practice […] RPAS uses by individuals, for private activities will normally be subject to Directive 95/46/EC requirements and will rarely benefit from the household exception.*"[112]

In arriving at this conclusion, the EDPS applied the criteria proposed by the Article 29 Working Party in its 2013 Statement. Specifically, it reasoned that

"*[…] processing carried out via RPAS might meet several of these criteria and fall out of the scope of the household exception. For example, personal data might be disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances. […] In addition, if RPAS were to be used for private purposes in public areas, it is likely that many individuals with no personal relationship with the pilot will see their data collected or even with the individuals accessing the data. The scale and frequency might vary a lot depending on hobbyists who could join clubs and associations and sometimes, but not necessarily and systematically, act in a collective and organised manner. The last criterion is even more relevant since there is an undeniable potential adverse impact on individuals, i.e. the intrusion into their privacy.*"[113]

The EDPS concluded that the use of RPAs by individuals for private activities would "quite frequently" be subject to the requirements of Directive 95/46/EC.[114] Of the five criteria proposed by the Article 29 Working Party, mainly the second (data subjects involved) and fourth (adverse impact) seem to weigh against application of the personal use

[110] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", *l.c.*, at paragraph 15.
[111] *Ibid*, at paragraphs 33 et seq.
[112] *Ibid*, at paragraph 68.
[113] *Ibid*, at paragraph 38.
[114] *Ibid*, at paragraph 39. The EDPS also added that, in any event, the processing of personal data will need to comply with other relevant rules in areas such as civil or criminal law, intellectual property, aviation or environmental law. (*Id.*)

exemption.[115] The two remaining criteria (publicity, scale and concerted action) might be relevant in specific cases, but not all. It is not clear from the EDPS opinion whether satisfying criteria (2) and (4) alone would be sufficient to hold the personal use exemption inapplicable. Will data protection law apply to every hobbyist? Or only if the hobbyist also flies it around the neighbourhood on a regular basis? The *Ryneš* ruling sheds some, albeit limited, light on this issue.

c. Implications of *Ryneš*

In *Ryneš*, the ECJ held that continuous video surveillance of a public space cannot be regarded as a "purely personal or household" activity. According to the Court, the monitoring of a public space meant that the surveillance system was "directed outwards from the private setting" and therefore did not fall within the scope of article 3(2).[116] The *Ryneš* ruling thus provides some additional support for the position of the EDPS. After all, as soon as a drone is flown outdoors, any sensors attached to the drone will generally be directed "outwards from the private setting". If the drone captures personal data, one could argue that its user is automatically subject to the requirements of Directive 95/46. One should, however, be cautious not to unduly extend the *Ryneš* holding. In its reasoning, the ECJ made indirect references to (1) the data subjects involved[117]; (2) the scale and frequency of the processing[118] and (3) the potential adverse impact on the fundamental rights and freedoms of others[119]. It is true that the "monitoring of a public space" was a determinative element of the ECJ's holding. Nevertheless, it is clear that that other elements influenced the Court's final holding[120] and therefore should not be discounted from future analyses.

[115] As the EDPS points out, a drone flying in a public space could significantly interfere with the privacy interests of others. And most likely much of the data captured would concern individuals who have no personal relationship whatsoever with the pilot.

[116] Court of Justice of the European Union, *František Ryneš v. Úřad pro ochranu osobních údajů*, C-212/13, 11 December 2014, at paragraph 33.

[117] The ECJ implicitly considered the data subjects involved by taking into account that the camera system also partially monitored a public place.

[118] The ECJ made repeated reference the "continuous" nature of the recording.

[119] See paragraph 29 of *Ryneš*: "*Since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter […] the second indent of Article 3(2) of that directive must be narrowly construed*." While the reference to the EU Charter serves to further the claim that article 3(2) should be construed narrowly, it is also suggests of a greater focus on impact or risk in determining the scope and meaning of the provisions of Directive 95/46 (as was also the case in the *Google Spain* ruling).

[120] The ECJ clearly qualified its reasoning, e.g. by referring to video surveillance "such as that at issue" in the proceedings (paragraph 35).

d. Evaluation

Policymakers around the world are still grappling with the question of how to regulate drones.[121] In some jurisdictions, specific rules governing drone usage have already been adopted.[122] In other jurisdictions, pre-existing rules partially or completely restrict certain types of drone usage.[123] In the EU, drones capturing personal data must, as a rule, comply with Directive 95/46. According to the EDPS, even hobbyists will ordinarily be subject to the requirements of Directive 95/46.[124] This may come as a surprise to the hobbyist playing with his drone in the park on a Sunday afternoon.[125] While the EDPS did not state that *all* hobbyists will be subject to data protection law, it did suggest that hobbyists would only "rarely" benefit from the personal use exemption. This conclusion is somewhat troubling. In my view, it is disproportionate to subject *all* drone hobbyists to the regulatory framework of Directive 95/45. First, many hobbyists have neither the intention nor desire to process the data of individuals, but do so purely on an "incidental" basis. Second, it seems excessive to require hobbyists to familiarize themselves with the requirements of Directive 95/46. A hobbyist should receive easily accessible and understandable guidelines, preferably integrated with other relevant legal requirements (e.g., respect no-fly zones, keep your drone within sight, do not film over/near other people's private property without their permission, etc.).[126] Of course, data protection authorities are ideally positioned to translate general requirements of data protection into specific guidance. There is, however, a qualitative difference between formally subjecting private individuals to data protection norms, versus publishing a list of guidelines for private uses of a particular technology. In the first scenario, it is up to every individual to familiarize him or herself with data protection law, submit notifications where applicable, negotiate contracts (e.g., if data captured by drones is stored in the cloud) and face legal uncertainty. In the second scenario, the

[121] See e.g., A. Parker, "The Drones of Chicago: More Hobbyists Hovering as Laws Try To Catch Up", DNAinfo Chicago, 9 September 2014, accessible at http://www.dnainfo.com/chicago/20140909/river-north/drones-of-chicago-more-hobbyists-hovering-as-laws-try-catch-up (last accessed 16 March 2015) and X., "Drone owners register called for by House of Lords", *BBC News Technology*, 5 March 2015, accessible at http://www.bbc.com/news/technology-31735662 (last accessed 16 March 2015)

[122] See e.g. R. De Peyer, "Drones are banned from Royal Parks amid 'fears over impact on wildlife and visitor safety'", *London Evening Standard*, 16 March 2015, accessible at http://www.standard.co.uk/news/london/drones-banned-from-royal-parks-amid-fears-over-impact-on-wildlife-and-visitor-safety-10095538.html (last accessed 16 March 2015).

[123] See e.g. KnowBeforeYouFly, "Recreational users", accessible at http://knowbeforeyoufly.org/for-recreational-users and www.dronelaw.net (last accessed 16 March 2015).

[124] The same viewpoint was defended by the Belgian Data Protection Authority: Commissie voor de Bescherming van de Persoonlijke levenssfeer, Advies nr 32/2015 van 22 juli 2015 betreffende het Ontwerp van Koninklijk besluit met betrekking tot het gebruik van op afstand bestuurde luchtvaarttuigen in het Belgisch luchtruim (CO-A-2015-030).http://www.privacycommission.be/sites/privacycommission/files/documents/advies_32_2015.pdf (last accessed 5 August 2015).

[125] In the US, drones are already being used by hobbyists (to take arial photographs, birdwatching or catching a glimpse of an outdoor festival) http://www.dnainfo.com/chicago/20140909/river-north/drones-of-chicago-more-hobbyists-hovering-as-laws-try-catch-up (last accessed 16 March 2015).

[126] See e.g. Academy of Model Aeronautics, "sUAS Flight Safety Guide", 2014, accessible at http://suas.modelaircraft.org/ama/images/sUAS_Safety_Program_web.pdf (last accessed 16 March 2015).

individual is told where the specific limits are and what the consequences are in case of non-compliance (e.g., liability in tort, administrative penalty).

Finally, we should also not lose sight of responsibilities which might be bestowed on the manufacturers of drones or other stakeholders. In its opinion, the EDPS made three recommendations to help ensure compliance, namely (1) generate a public debate by raising awareness on the privacy implications of RPAs; (2) support implementation of privacy by design by RPA manufactures; and (3) assist controllers with compliance.[127] These measures, combined with traditional remedies such as tort law, trespass etc. may go a long way in curbing inappropriate drone usage without formally subjecting individuals acting in a private capacity to the full range of data protection requirements.

5.3 Google Glass

a. "Far from dead"

Project Glass was officially announced by Google in April of 2012.[128] Its objective was to build a technology which "*helps you explore and share your world, putting you back in the moment*"[129]. Google Glass is a "wearable", controllable either through voice commands, a touchpad (which is located on the side of the device) and/or smartphone application.[130] It features a camera, an optical display and, of course, internet connectivity. One of the ideas behind Google Glass is to allow users to capture and augment their reality seamlessly. No more looking down at your phone to check for incoming messages. No more having to stop what you're doing to take out your camera (or, for that matter, run a Google search).[131]

Google Glass is not yet available in retail stores. Initially, the device was only available to "Explorers", which have been described as "*a select group of geeks and journalists who paid $1,500 for the privilege of being an early adopter*".[132] Later, the company began organizing public events and actively encouraging application development by third parties. Notwithstanding headlines suggesting that Google Glass has been "shut down", it is expected that the device will eventually still become a mass consumer product.[133]

---

[127] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", *l.c.*, at paragraphs 56 et seq.

[128] See Glass Almanac, "The History of Google Glass", accessible at http://glassalmanac.com/history-google-glass (last accessed 16 March 2015).

[129] Google Glass, "Google Glass", 4 April 2012, accessible at https://plus.google.com/+GoogleGlass/posts/aKymsANgWBD (last accessed 16 March 2015).

[130] See http://en.wikipedia.org/wiki/Google_Glass

[131] Based on S. Brin, "Why Google Glass", TED, February 2013, accessible at http://www.ted.com/talks/sergey_brin_why_google_glass?language=en (last accessed 16 March 2015).

[132] N. Bilton, "Why Google Glass Broke", New York Times, 4 February 2015, accessible at http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html?_r=0 (last accessed 16 March 2015).

[133] See e.g. C. Metz, "Sorry, But Google Glass isn't anywhere close to dead", Wired, 8 February 2015, accessible at http://www.wired.com/2015/02/sorry-google-glass-isnt-anywhere-close-dead; X., "Google to 'start again'

b. Facial recognition

In May 2013, Google announced that it will not, for the time being, approve any application for Google Glass that involves facial recognition:

> "*As Google has said for several years, we won't add facial recognition features to our products without having strong privacy protections in place. With that in mind, we won't be approving any facial recognition Glassware at this time*."[134]

Just two weeks prior to the announcement, a third-party developer published *MedRef*, which claimed to be "*the first app for Google Glass with facial recognition*".[135] *MedRef* would allow doctors to "*create patient folders by voice, add photo and voice notes, view previous notes, and also find patient folders by facial recognition*".[136] But why stop there? While Google professed it would not approve facial recognition apps for the time being, this didn't stop third-party developers. The most well-known example is probably "Facial Network", the US company behind "Nametag". Nametag

> "*can spot a face using Google Glass' camera, send it wirelessly to a server, compare it to millions of records and in seconds return a match complete with a name, additional photos and social media profiles*." [137]

Facebook, for its part, has recently sent Facial Network a cease and desist letter to stop it from harvesting user data, claiming it violated Facebook's terms of use.[138]

In 2008, Jonathan Zittrain mused about the implications of apps like Nametag as follows:

> "*With reputation systems already advising us on what to buy, why not have them also help us make the first cut on whom to meet, to date, to befriend? […] These systems*

---

with Glass", *BBC News Technology*, 6 February 2015, accessible at http://www.bbc.co.uk/news/technology-31164840 (last accessed 16 March 2015).

[134] Google Glass, "Glass and Facial Recognition", 1 June 2013, accessible at https://plus.google.com/u/0/+GoogleGlass/posts/fAe5vo4ZEcE (last accessed 16 March 2015).

[135] See Google Glass Apps, "MedRef Google Glass App", http://glass-apps.org/medref-google-glass-app, last accessed 16 March 2015 (note: this is not an "official" Glassware directory).

[136] Id.

[137] See http://www.nametag.ws. Facial Network is hopeful Google will eventually reconsider: "*Google has announced that facial recognition will not yet be supported for Glass; undoubtedly due to pressure from privacy groups but FacialNetwork.com believes that by providing applications with such vast societal benefits, Google will eventually reconsider*" (*Ibid*, last accessed 16 March 2015). A companion app, called "Creepshield", would allow you to check if the person in front of you is a registered sex offender. See C. Poladian, "NameTag: Facial Recognition App Checks If Your Date Is A Sex Offender But Should You Use It?", *International Business Times*, 14 January 2015, accessible at http://www.ibtimes.com/nametag-facial-recognition-app-checks-if-your-date-sex-offender-should-you-use-it-1539308 (last accessed 16 March 2015).

[138] M. McGee, "NameTag App Creators: We Got a C&D From Facebook", Glass Almanac, 12 September 2014, accessible at http://glassalmanac.com/nametag-app-creators-got-cd-facebook/5876 (last accessed 16 March 2015). In the meantime, Facebook continues its work on its own "DeepFace" project: See J. Bohannon, "Facebook will soon be able to ID you in any photo", Science Magazine, 5 February 2015, accessible at http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo.

can indicate who has not offered evidence that he or she is safe to meet —as is currently solicited by some online dating sites—or it may use Amazon-style matching to tell us which of the strangers who have just entered the café is a good match for people who have the kinds of friends we do. […] With enough people adopting the system, the act of entering a café can be different from one person to the next: for some, the patrons may shrink away, burying their heads deeper in their books and newspapers. For others, the entire café may perk up upon entrance, not knowing who it is but having a lead that this is someone worth knowing. Those who do not participate in the scheme at all will be as suspect as brand new buyers or sellers on eBay." [139]

c. Implications of *Ryneš* and *Google Spain*

Lorna Woods has already highlighted the potential implications of the *Ryneš* ruling for Google Glass:

"*If we take the approach that even partial public use of a fixed CCTV system cannot benefit from the household exception, still less would a portable, possibly inconspicuous device the purpose of which is uncertain. The reasoning seems stronger still if we consider the possible onward use of such data – via a website for example […] – taking into account the view in Lindqvist. Here it is less clear to see that the legitimate interests of the data controller (i.e. the person using the device to record and store personal data), assuming the processing were to be deemed 'necessary' to pursue that interest, would weigh heavily against a high level of protection for data protection even as between individuals.*"[140]

In other words: the argument can be made that users of Google Glass will be subject to the requirements of Directive 95/46, even when acting in a private capacity. *Ryneš* does not, however, categorically exclude the applicability of the personal use exemption here. Other than stealth, taking a picture using Google Glass is not all that different from taking a picture with one's smartphone (especially if Google Glass were to come equipped with a shutter sound or camera light). Of course, the act of uploading that same picture to the Web or making use of facial recognition software would require separate analysis.

When it comes to facial recognition applications, one should also take into account the implications of the *Google Spain* ruling.[141] *Google Spain* supports the premise that the providers of such services would be considered as "controllers" within the meaning of Directive 95/46/EC. As such, it is up to them to ensure the requirements of the Directive are

[139] J. Zittrain, *The Future of the Internet— And How to Stop It*, *o.c.*, p. 219-220.
[140] L. Woods, "Bringing Data Protection Home? The CJEU rules on data protection law and home CCTV", EU Law Analysis Blog, 11 December 2014, accessible at http://eulawanalysis.blogspot.be/2014/12/bringing-data-protection-home-cjeu.html (last accessed 16 March 2015).
[141] Court of Justice of the European Union, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C–131/12, 13 May 2014.

complied with. While a "general purpose" search engine might be able to avail itself of article 7(f) to engage in the indiscriminate collection of data on the web, a search engine dedicated to people searches using facial recognition arguably can't. Such service providers may reasonably be expected to verify compliance with all data protection requirements prior to making the service available to the public at large.

d. Evaluation

Regulating private uses of Google Glass through data protection law raises significant questions of proportionality. First, as with the drone hobbyist, it seems unreasonable to expect the average user of Google Glass to apply the analytical framework of Directive 95/46 on a daily basis.[142] Second, alternative regulatory strategies may actually be more effective. It is likely that more results will be achieved by bringing enforcement actions against service providers that offer privacy-intrusive applications - as opposed to focusing on the users of such the technologies. Of course, even if data protection authorities strictly enforce data protection requirements against the providers of applications and/or operating systems[143], certain individuals will still be able to make use of privacy-intrusive technologies. But for this scenario, it may be more useful to institute generic provisions in civil and criminal codes rather than mandating wholesale application of data protection law. For example, several European countries restrict not only the sale but also the use of tools designed to violate one's confidentiality of communications (e.g. mobile spyware).[144] Finally, nothing prevents the judiciary from taking into account data protection considerations in the further development of "privacy torts"[145]. Through the principles of "privacy by design" and "privacy by default", regulators might well be able to reduce mainstream misuses of personal data. For those that persist, simple inserts in the criminal or civil code or the extension of existing legal constructs (e.g. tort law, the right to control the use of one's image, breach of confidence, misuse of private information) may be enough to fill the gaps.

---

[142] Contra: Opinion of Advocate-General Jääskinen, František Ryneš v Úřad pro ochranu osobních údajů, Case C-212/13, 10 July 2014, at paragraph 66 ("*It is illogical to argue that, in order to protect Mr Ryneš' fundamental rights, it is appropriate to leave unapplied an EU directive which is specifically intended to strike a fair balance between Mr Ryneš' rights and the rights of other natural persons, namely, the people affected by the processing of personal data.*")

[143] See also Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", WP 202, 27 February 2013, p. 9 et seq.

[144] See e.g. article 550bis of the Belgian Criminal Code. See also J. Kerkhofs and P. Van Linthout, "Cybercriminaliteit doorgelicht", T. Strafr., 2010/4, p. 185 et seq.

[145] See e.g. High Court of Justice in Northern Ireland, Queen's Bench Division, CG v Facebook Ireland and Joseph McCloskey, No [2015] NIQB 11, STE9491, 20 February 2015, accessible at http://www.bailii.org/nie/cases/NIHC/QB/2015/11.html (last accessed 5 August 2015). See also Section 652 of the Restatement (Second) of Torts (1977), accessible at http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm (last accessed 16 March 2015).

6. The role of Data Protection Authorities

Perhaps the most compelling argument against extending the scope of the personal use exemption concerns the need for effective redress. Directive 95/46 requires Member States to provide an independent supervisory authority which is dedicated to monitoring compliance.[146] It also stipulates that every individual should have the right to file a complaint if they feel their rights and freedoms are being harmed by personal data processing.[147] From the perspective of an aggrieved individual, filing a complaint with a national DPA constitutes a much lower threshold than the initiation of formal legal proceedings. While the former can often be done online, free of charge, the latter is likely to entail considerable legal expense. The matter of DPA oversight is an important one, which also raises its own questions regarding proportionality. As noted by the Working Party:

> "*It is certainly the case that an inappropriate level of scrutiny and regulation of natural persons' personal or household processing activities by DPAs could inhibit individuals' freedom of speech and could in itself constitute a breach of the individual's right to privacy*."
> *[…]*
> "*However, data protection authorities are also experiencing an increasing number of complaints emanating from individuals' personal use of the internet. A typical complaint might be that a pupil has used a social networking site to say post a derogatory, inaccurate or hurtful message about a teacher. Currently some data protection authorities would reject any complaints about the pupil on the grounds that the processing of personal data involved would fall within the personal or household processing exemption. Some data protection authorities also take the view that other elements of the law – for example those relating to libel or harassment – are more appropriate instruments for dealing with issues such as 'cyber-bullying'. It is the case though that some DPAs do – increasingly – take on the role of mediating individuals' internet postings*"[148]

The fragments quoted above illustrate the difficult choice that lies ahead. On the one hand, exempting individuals may leave victims of privacy harms without DPA assistance. On the other hand, too much regulatory scrutiny of "private" processing activities would be disproportionate. But what if there was a middle ground? Article 28(4) of Directive 95/46 provides that

[146] Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.*, p. 1
[147] *Ibid*, p. 3.
[148] *Ibid*, p. 2 and 3.

"Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data."

The scope of article 28(4) is extremely broad. It allows DPAs to hear any complaint where an individual's rights and freedoms are affected by the processing of personal data.[149] Of course, the enforcement powers of DPAs are generally confined to processing activities which fall within the scope of data protection law. Still, nothing prevents DPAs from acting as "ombudsmen" or "mediators" for claims against private individuals. DPAs can also issue opinions on their own initiative as to how privacy interests might be safeguarded in relation to specific technological developments. DPAs can also play a role regarding education and awareness, even if the processing activity formally falls outside the scope of data protection law.[150] As noted by the Working Party, when considering the relevance of legal remedies other than data protection law:

"*Whilst DPA's can have no formal role in enforcing these laws, they should – as far as is practicable – be prepared advise* [sic] *individuals as to other sources of redress when they are the victims of personal data processing that falls within the scope of the personal and household processing exemption. DPA's should also continue to monitor the situation closely and if there is evidence that individuals are going unprotected from serious harm, WP29 should be prepared to issue an opinion as to how the situation might be rectified. DPA's should also continue to work with leading player in the industry – for example social networking companies and search-engines – to make it easier for individuals to have malicious or damaging content taken down from the internet*."[151]

Data protection authorities will have the power to investigate whether the personal use exemption can be applied in particular instance.[152] Enforcement by DPAs should not, however, extend to individuals using technology in a private capacity.

[149] Strictly speaking, it is not even necessary that the processing affects the right to privacy or data protection.
[150] Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.,* p. 6
[151] Ibid, p. 7-8.
[152] Ibid, p. 1 and 4-5

7. Conclusion

It is time to broaden the scope of the personal use exemption. Already today, a clear mismatch exists between the legal obligations of "controllers" and the online practices of individuals. People share, tweet, tag and pin personal data whilst blissfully unaware of the strictures of data protection law. Formally applying the requirements of Directive 95/46 to these activities by default would be disproportionate. More often than not, it would also be impractical and artificial.

The ECJ has consistently held that Directive 95/46 does not, by itself, unduly restrict legitimate uses of technology. While the Directive supports a certain degree of flexibility, it is clear that the existing notion of "purely personal or household activities" is overly narrow. Absent further derogations, there is a risk that data protection law will unduly interfere with individual freedom. In my view, the personal use exemption should simply apply to all activities which may reasonably be construed as taking place in the course of an individual's private or family life.[153] In addition, an individual should be able to benefit from the personal use exemption regardless of the recipients involved.[154] Furthermore, while the location or direction of a recording device *can* be a relevant factor, it need not be determinative. Instead, the terms "private and family life" should (continue to) be interpreted broadly, extending to any activities related to the development of one's personal identity or the establishment of relationships with others.[155] Only when the risk of excessive interference in the privacy interests of others is evident (e.g., due to the scale or frequency of the processing, combined with the recipients and nature of the data), might it be proportionate to bring the activities of private individuals within the scope of data protection law. In order to promote legal certainty, additional criteria establishing the boundaries of the personal use exemption should be anchored in the law.

The EU institutions are currently in the process of deciding the future of the personal use exemption. Overall, the proposed changes seem to be heading in the right direction. The criteria proposed by Article 29 Working Party provide useful additional guidance, while at the same time supporting a certain degree of flexibility. The Council has proposed to drop the word "exclusively", which would encourage a broader understanding of the personal use exemption. Most important of all, however, is the change in mind set. Data protection law is not the only instrument which offers protection misuse of personal data. Other legal constructs, such as tort law and personality rights, are better suited to regulate conflicts

[153] The first part of the "personal use" test promulgated by the ECJ in *Lindqvist* also refers to "in the course of private or family life of individuals" (Case C-101/01, at paragraph 74).
[154] This would effectively require reversing the second part of personal use test advanced by *Lindqvist*.
[155] The European Court of Human Rights has underlined that it also protects a right to identity and personal development, and the right to establish and develop relationships with others. (European Court of Human Rights, *P.G. and J.H. v. United Kingdom*, 25 September 2001, application no. 44787/98, paragraph 56 and European Court of Human Rights, *Niemietz v. Germany*, 16 December 1992, application no. 13710/88, paragraph 29; available at http://www.echr.coe.int).

between private individuals. It is up all of us to develop these constructs further, and to inform them with data protection considerations as needed.

Acknowledgements

The author would like to thank Peggy Valcke, Els Kindt, Geertrui Van Overwalle and Damian Clifford for their valuable comments and feedback. The research leading to this paper has received funding from the agency for Innovation by Science and Technology (www.iwt.be) in the context of the project "Security and Privacy for Online Social Networks" (www.spion.me), the Flemish research institute iMinds (www.iminds.be) and the European Community's Seventh Framework Programme for research, technological development and demonstration in the context of the REVEAL project (www.revealproject.eu) (grant agreement no: 610928).